



Docket No.: S&ZIO020405

IPW

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

By:  Date: February 15, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applic. No. : 10/713,692 Confirmation No: 2918
Applicant : Angela Engels, et al.
Filed : November 14, 2003
Art Unit : 2621
Examiner : Kim, Chong R
Title : METHOD FOR FORGERY RECOGNITION IN FINGERPRINT
RECOGNITION BY USING A TEXTURE CLASSIFICATION OF
GRAY SCALE DIFFERENTIAL IMAGES
Docket No. : S&ZIO020405
Customer No. : 24131

CLAIM FOR PRIORITY

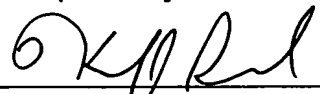
Commissioner for Patents,
P.O. Box 1450, Alexandria, VA 22313-1450

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 101 23 330.2, filed May 14, 2001.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,


Kerry P. Bisselman
Reg. No. 37,237

Date: February 15, 2007
Lerner Greenberg Sterner LLP
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101
/sa

BUNDESREPUBLIK DEUTSCHLAND



CERTIFIED COPY OF
PRIORITY DOCUMENT

Prioritätsbescheinigung DE 101 23 330.2 über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 23 330.2

Anmeldetag: 14. Mai 2001

Anmelder/Inhaber: Infineon Technologies AG, 81669 München/DE

Bezeichnung: Verfahren zur Fälschungserkennung bei der Finger-
abdruckerkennung unter Verwendung einer Textur-
klassifikation von Grauwertdifferenzbildern

IPC: G 06 K 9/36

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe
der Teile der am 14. Mai 2001 eingereichten Unterlagen dieser
Patentanmeldung unabhängig von gegebenenfalls durch das Kopier-
verfahren bedingten Farbabweichungen.

München, den 30. Januar 2007
Deutsches Patent- und Markenamt
Der Präsident

Im Auftrag


Brosig

Beschreibung

Verfahren zur Fälschungserkennung bei der Fingerabdruckerken-
nung unter Verwendung einer Texturklassifikation von Grau-
5 wertdifferenzbildern

Die vorliegende Erfindung bezieht sich auf ein Verfahren zur
Fälschungserkennung bei der Fingerabdruckerkennung unter Ver-
wendung einer Texturklassifikation von Grauwertdifferenzbil-
10 dern und insbesondere auf ein Verfahren zur Fälschungserken-
nung bei der Fingerabdruckerkennung auf der Grundlage einer
Bildsequenz. Insbesondere bezieht sich die vorliegenden Er-
findung auf ein dynamisches, Software-basiertes Verfahren zur
Fälschungserkennung.

15

Die Fingerabdruckerkennung ist eine zuverlässige und weit
verbreitete Technik zur Personenidentifikation. Im Stand der
Technik sind verschiedene Verfahren zur Erkennung von Finger-
abdrücken bekannt, wobei zunächst die einfachen Bilderken-
20 nungsverfahren zu nennen sind, die bei Auflegen eines Fingers
ein Bild desselben erfassen und mit abgespeicherten Bildern
vergleichen, um eine Person zu identifizieren.

Der Nachteil dieser Verfahren besteht darin, dass diese recht
25 leicht zu täuschen sind, beispielsweise durch das Auflegen
eines Silikonabgusses einer Fingerkuppe oder ähnlichem. Fer-
ner ist bei diesen Verfahren der große Speicherbedarf für die
verwendeten Vergleichsbilder („Templates“) sowie der große
Rechenaufwand nachteilhaft. Der Nachteil der leichten Täu-
30 schung existiert auch bei minutien-basierten Verfahren.

Zur Lösung dieser Problematik wurde im Stand der Technik vor-
geschlagen, Merkmale aus den Fingerabdrücken zu extrahieren
und die Erkennung auf der Grundlage dieser Merkmale durchzu-
35 führen. Bekannte biometrische Verfahren für die Personener-
kennung können beispielsweise in automatisierten Systemen
implementiert werden. Solche Systeme verarbeiten die Eingabe-

daten, die die biometrischen Merkmale enthalten, und extrahieren charakteristische Merkmale, die anschließend einer Person zugeordnet werden können.

5 Für eine zuverlässige Personenzuordnung ist jedoch sicherzustellen, dass auf dem Signalpfad zwischen dem zu messenden Objekt und der Bildaufnahmeeinheit keine Manipulation möglich ist.

10 Bei der Erkennung von Fingerabdrücken durch ein automatisches System zur Fingerabdruckerkennung sind also Verfahren erforderlich, die nur von echten Fingern erzeugte Bilder zu der Verarbeitungseinheit weiterleiten und eventuell die von Imi-

15 Im Stand der Technik bekannte Ansätze zur Lösung dieser Problematik werden nachfolgend kurz erläutert, wobei hier zwischen Hardware-basierten Lösungen und Software-basierten Lösungen unterschieden wird.

20 Eine erste Lösung besteht darin, den Sensor, mittels dem der Fingerabdruck zu erfassen ist, um integrierte oder externe Hardware-Komponenten zu ergänzen. Solche bekannten Lösungen erfassen beispielsweise eine Impedanz der aufliegenden Finger, wie dies im US Patent 5,953,331 näher beschrieben wird. Andere technische Realisierungen von Hardware-basierten Fälschungserkennungen umfassen eine Feuchtigkeitsmessung, eine Pulsmessung und eine Druckmessung.

30 Neben den Hardware-basierten Lösungen sind auch Lösungen bekannt, bei denen die vom Sensor kommenden Daten zur Fälschungserkennung mittels Software ausgewertet werden. Bei der Software-basierten Fälschungserkennung wird zwischen statischen und dynamischen Verfahren unterschieden.

35 Bei den statischen Verfahren wird nur ein Bild ausgewertet, üblicherweise jenes, das auch zur Erkennung benutzt wird.

Statische Software-basierte Fälschungserkennungsverfahren basieren beispielsweise auf der Auswertung von Fingerabdruckbildern, die als Bitmap mit Grauwerten vorliegen. Andere Software-basierte, statische Verfahren werten die im Bild sichtbaren Talgdrüsen aus.

Bei den dynamischen Verfahren wird eine Sequenz aufeinanderfolgender Bilder des Sensors, die den Vorgang des Finger-Auflegens beschreiben, verwendet. Eine dynamische Fälschungserkennung erhöht die Erkennungs- und Fälschungssicherheit biometrischer Fingerabdrucksysteme, bei denen zusätzlich z. B. eine Bewegung der Person, ein Druck, mit dem der Finger aufgelegt wird, oder Schweiß auf dem Finger bei der Erkennung herangezogen werden. Andere dynamische Verfahren entnehmen die entsprechenden Informationen zur Fälschungserkennung aus Sequenzen von Fingerabdruckbildern.

Die oben beschriebene dynamische softwarebasierte Lösung zur Fälschungserkennung, bei der aus Sequenzen von Fingerabdruckbildern entsprechende Informationen zur Fälschungserkennung herausgezogen werden, basiert auf der großflächigen Verformung der Haut und damit des Fingerabdrucks, was als „Makroelastizität“ bekannt ist. Der Nachteil der Ausnutzung der Makroelastizität besteht darin, dass sichtbare Unterschiede zwischen Originalfingern und Fälschungen im allgemeinen erst dann erkannt werden können, wenn der Finger oder die Fälschung mit erheblichem Druck aufgelegt werden.

Ausgehend von diesem Stand der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein verbessertes Verfahren zur Fälschungserkennung zu schaffen, bei dem sicher zwischen einem echten Fingerabdruck und einem gefälschten Fingerabdruck unterschieden werden kann, ohne dass der Abdruck unter Berücksichtigung bestimmter Randparameter, wie z. B. des Anpressdruckes, erzeugt werden muss.

Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1 gelöst.

Die vorliegende Erfindung schafft ein Verfahren zur Fälschungserkennung, mit folgenden Schritten:

(a) Erfassen einer Bildsequenz, die eine Mehrzahl von Bildern des zu erkennenden Fingerabdrucks umfasst;

10 (b) Bilden zumindest eines Differenzbildes aus zwei Bildern der erfassten Bildsequenz;

(c) Erfassen einer Textur in dem zumindest einen Differenzbild; und

15

(d) Vergleichen der Textur mit einer vorbestimmten Textur, um zu bestimmen, ob die erfasste Bildsequenz von einem echten Finger oder von einem Imitat stammt.

20 Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, dass die in einer Bildsequenz sichtbare Bewegungscharakteristik beim Fingerauflegen zu einem erheblichen Teil durch die Elastizität des Fingers, insbesondere der Haut, bedingt ist. Hierbei werden die nachfolgend genannten zwei Arten von Elastizität unterschieden.

25 Zum einen existiert die bereits oben erwähnte Makroelastizität, die die großflächige Verformung der Haut und damit des Fingerabdrucks beschreibt, und die die oben erwähnten Nachteile mit sich bringt. Demgegenüber steht die „Mikroelastizität“, die die Verformung der Fingerlinien beim einfachen Auflegen des Fingers, beispielsweise auf eine Sensoreinheit, beschreibt.

30 Originalfinger und gefälschter Finger („Fälschung“) unterscheiden sich sowohl in der Mikro- als auch in der Makroelastizität, die beide in einer Bildsequenz des Auflegvorgangs

sichtbar sind und zur Fälschungserkennung durch den erfindungsgemäßen Bildverarbeitungsalgorithmus analysiert werden. Bei der Erfassung der Makroelastizität kann beispielsweise ein Linienwachstum der Fingerlinien erfasst werden.

5

Sichtbare Unterschiede zwischen Originalfingern und Fälschungen ergeben sich für die Makroelastizität erst dann, wenn Finger oder Fälschung mit erheblichen Druck aufgelegt werden. Um diesen Nachteil zu vermeiden und um sicherzustellen, dass eine Bildsequenz ohne Mitwirkung der zu identifizierenden Person erfolgt, nämlich nur durch das einfache Auflegen des Fingers, hat die vorliegende Erfindung erkannt, dass dies durch eine Analyse der Mikroelastizität erreicht werden kann.

10

15

Die Mikroelastizität zeigt sich in der zeitlichen Veränderung der Fingerlinien beim Auflegen. Hierbei ist zu beobachten, dass die Fingerlinien vom originalen Finger beim Auflegen sowohl breiter als auch dunkler werden, was bei gefälschten Fingern nicht im gleichen Maß der Fall ist.

20

Der Vorteil der vorliegenden Erfindung besteht darin, dass die Betrachtung der Mikroelastizität es ermöglicht, auf sichere Weise zwischen Bildsequenzen von Originalfingern und Fälschungen zu unterscheiden, da die Mikroelastizität eine wesentliche und schwer fälschbare Eigenschaft ist.

25

30

Gemäß der vorliegenden Erfindung wird eine Texturklassifikation von Grauwertdifferenzbildern von zeitlich aufeinanderfolgenden Bildern einer Bildsequenz durchgeführt. Anhand des Klassifikationsergebnisses lässt sich eine Fälschung von einem Original unterscheiden.

35

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend anhand der beiliegenden Figuren näher erläutert. Es zeigen:

Fig. 1A eine Bildsequenz, die dem erfindungsgemäßen Verfahren zugrunde liegt;

Fig. 1B eine schematische Darstellung einer Sensoreinheit;

5

Fig. 2A und 2B ein Flussdiagramm, das ein bevorzugtes Ausführungsbeispiel des erfindungsgemäßen Verfahrens darstellt;

10

Fig. 3 zeigt verschiedene Darstellungen von aufeinanderfolgenden Bildern und entsprechenden Differenzbildern für einen Originalfinger, eine Folienfälschung und eine Hauchfälschung; und

15

Fig. 4 ein Flussdiagramm, das ein Ausführungsbeispiel einer Texturklassifikation gemäß der vorliegenden Erfindung näher erläutert.

20

In Fig. 1A ist mit 100 eine beispielhafte Bildsequenz gezeigt, die dem erfindungsgemäßen Verfahren zur Fälschungserkennung von Fingerabdrücken zugrunde liegt. Wie zu erkennen ist, umfasst die Bildsequenz 100 eine Mehrzahl von Einzelbildern 0 bis 19, wobei die Einzelbilder 0 bis 19 in der Bildsequenz 100 zeitlich aufeinander folgen, wie durch den Pfeil 102 dargestellt ist. Die Bildsequenz 100 enthält vorzugsweise Einzelbilder als Bitmaps mit Grauwerten. Die Bildsequenz 100 wird während des Auflegens eines Fingers 104, wie in Fig. 1B gezeigt ist, durch eine Sensoreinheit 106 erfasst. Es ist darauf hinzuweisen, dass die Bildsequenz 100 nicht während des Aufliegens des Fingers auf der Sensoreinheit 106 sondern beim Auflegen des Fingers 104 auf den Sensor 106 erfasst wird, wie auch aus den Einzelbildern 0 bis 19 zu erkennen ist. Genauer gesagt zeigen die Bilder 0 bis 6 überhaupt keinen Finger und erst ab dem Bild 7 ist zu erkennen, dass sukzessive immer größere Flächen des Bildes vom Finger bedeckt sind.

35

Wenn die Bilder einer Bildsequenz von einem echten Finger stammen, vergrößert sich die Auflagefläche während des Auflegvorgangs über mehrere Bilder. Wenn die Bilder der Bildsequenz von einer Fälschung stammen, erscheint der Fingerabdruck ohne Übergang gleich mit der vollen Auflagefläche. Ferner ändert sich bei den echten Fingern in den Bildern nach dem Sichtbarwerden noch der Kontrast und die Breite der Fingerlinien. Bei einer Fälschung bleibt beides in den Bildern weitgehend unverändert. Die gerade erwähnten Effekte resultieren aus der unterschiedlichen Elastizität von Finger und Fälschung.

Gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung wird aus einer Sequenz von Grauwertbildern, die den zu erkennenden Fingerabdruck aufweisen, zunächst eine Sequenz von Differenzbildern berechnet, indem jeweils zwei aufeinanderfolgende Bilder der Sequenz Pixelweise voneinander subtrahiert werden. In den Differenzbildern sind zu geeigneten Zeitpunkten in der Bildsequenz, vor allem zum Zeitpunkt des ersten Kontakts zwischen dem Finger 104 und dem Sensor 106 (siehe Fig. 1B), unterschiedliche Texturen zu erkennen, je nach dem, ob die Bildsequenz von einem Originalfinger oder von einer Fälschung stammt. Dies spiegelt die unterschiedliche Mikroelastizität von Finger und Fälschungsmaterialien wieder. Anhand einer Texturklassifikation der Grauwertdifferenzbilder wird bestimmt, ob die Sequenz von einem Originalfinger oder von einer Fälschung stammt.

Anhand der Fig. 2 wird nachfolgend ein erstes bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung näher erläutert. Aus der erfassten Bildsequenz wird immer eine Differenzbildsequenz erzeugt. Aus dieser Differenzbildsequenz muss ein besonders charakteristisches Differenzbild herausgesucht werden. Dazu werden in aufsteigender Folge der Differenzbildsequenz zunächst Gradientenbilder und anschließend die Histogramme der Gradientenbilder berechnet. Von den Histogrammen wird der Schwerpunkt bestimmt. Überschreitet

dieser Schwerpunkt eine Schwelle, so wird das entsprechende Histogramm für die nachfolgende Fälschungserkennung herangezogen.

5 In Fig. 2A ist der Schritt 200 gezeigt, in dem beispielsweise die in Fig. 1A gezeigte Bildsequenz 100 bestehend aus den Bildern 0 bis 19 erfasst wird, die den zu erkennenden Fingerabdruck darstellen. Im nachfolgenden Schritt 202 wird ein Differenzbild aus zwei aufeinanderfolgenden Bildern, beispielsweise durch Pixelweise Subtraktion von zwei aufeinanderfolgenden Grauwertbildern der Bildsequenz erzeugt. Im Schritt 204 wird bestimmt, ob weitere Differenzbilder zu erfassen sind oder nicht. Falls der Schritt 204 bestimmt, dass weitere Differenzbilder zu erfassen sind, kehrt das Verfahren zum Schritt 202 zurück, ansonsten geht das Verfahren zum Schritt 206. Im Schritt 206 wird aus der Differenzbildsequenz eine Textur ausgewählt, die anschließend, wie in Fig. 2B gezeigt ist, in einem Schritt 208 mit einer vorbestimmten Textur verglichen wird. Stimmen die Texturen überein, so geht das Verfahren zum Schritt 210, in dem bestimmt wird, dass der Fingerabdruck echt ist, also die Bildsequenz von einem echten Finger her stammt. Wird im Schritt 208 festgestellt, dass die Texturen nicht gleich sind, so wird im Schritt 212 festgestellt, dass der Fingerabdruck nicht echt ist, die Bildsequenz also von einer Fälschung stammt.

Die oben beschriebene Erzeugung von Differenzbildern im zweiten Schritt 202 wird nachfolgend anhand der Fig. 3 nochmals näher erläutert. In Fig. 3 ist ein aktuelles Bild 220a einer Bildsequenz gezeigt, die von einem Originalfinger stammt. Mit 220b ist ein in der Sequenz vorhergehendes Bild bezeichnet. Eine Pixelweise Subtraktion der Bilder 220a und 220b ergibt das Differenzbild 220c.

35 In Fig. 3 ist ferner ein Bild 230a gezeigt, welches ein aktuelles Bild einer Bildsequenz ist, die von einer Folienfäls-

sung her stammt. 230b bezeichnet das in der Sequenz vorhergehende Bild und das Differenzbild ist mit 230c bezeichnet.

5 Mit 240a ist ein aktuelles Bild einer Bildsequenz gezeigt, die von einer Hauchfälschung her stammt. Ein vorhergehendes Bild 140b ist gezeigt, das Differenzbild ist mit 240c bezeichnet.

10 In Fig. 3 sind jeweils Bilder 220a, 220b, 230a, 230b, 240a, 240b gezeigt, die horizontal die volle Auflösung haben (224 Pixel). Vertikal liegt nur $\frac{1}{4}$ der möglichen Auflösung vor (72 von 288 Pixel). Es wird nur $\frac{1}{4}$ des Sensorbildes ausgelesen, um so schnelle zeitliche Änderungen in der Bildsequenz sichtbar zu machen (ein Vollbild des Sensors kann in ca. 1/10 Sekunde
15 ausgelesen werden, ein Viertelbild entsprechend 4 mal schneller). Sichtbar ist also jeweils nur der Randbereich der Fingerabdruckbilder. Die Bilder sind aus Darstellungsgründen in vertikaler Richtung gedehnt, so dass die Fingerlinien verzerrt erscheinen.

20

Die Differenzbilder 220c, 230c, 240c zeigen jeweils das charakteristische Wachstum eines Fingerabdrucks während des Auflegevorgangs.

25 Beim Originalfinger 220c ist zu erkennen, dass zunächst einmal der Bereich, in dem Fingerlinien zu finden sind, in grober Näherung kreisförmig nach außen hin zunimmt (die Auflagefläche des Fingers nimmt zu). Außerdem ist zu erkennen, dass die einzelnen Fingerlinien breiter werden (sie bekommen im
30 Differenzbild einen dunklen Rand).

Bei der Folienfälschung 230c erweitert sich der Fingerabdruckbereich weitgehend geradlinig, was dem Abrollen der Folie auf dem Sensor entspricht. Außerdem ist kein Wachstum der
35 Fingerlinien (Ridges) zu erkennen (keine Ränder an den Fingerrillen).

Bei der Hauchfälschung 240c sind sowohl kein Wachstum des Fingerabdrucksbereich als auch kein Wachstum einzelner Fingerlinien (Ridges) zu erkennen (das Differenzbild 240c ist nur sehr schwach und gleichmäßig).

5

Die Differenzbilder 220c, 230c und 240c unterscheiden sich somit deutlich voneinander, so dass anhand derselben eine Unterscheidung zwischen einer Bildsequenz, die von einem Originalfinger her stammt und einer Bildsequenz, die von einer Fälschung her stammt, durchgeführt werden kann.

10

Anhand der Fig. 4 wird nachfolgend ein Beispiel für die Texturklassifikation der erzeugten Grauwertdifferenzbilder näher beschrieben.

15

Im Schritt 250 wird zunächst die erzeugte Grauwertdifferenzbildsequenz gefiltert, um eine Gradientenbildsequenz zu erhalten. Gemäß einem bevorzugten Ausführungsbeispiel erfolgt die Filterung anhand eines Sobelfilters.

20

Im nachfolgenden Schritt 252 werden für die erzeugte Gradientenbildsequenz Histogramme für die einzelnen Gradientenbilder berechnet. Im Schritt 253 wird ein geeignetes Histogramm selektiert. Anschließend erfolgt im Schritt 254 eine Korrelation des selektierten Histogramms mit vorgegebenen Masken bzw. Templates, wobei ein erstes Template bzw. eine erste Maske für einen Originalfinger und ein zweites Template bzw. eine zweite Maske für eine Fälschung vorgesehen ist. Im Schritt 256 wird bestimmt, ob ein Wert für die Korrelation mit dem Originalfinger-Template größer als der Wert für die Korrelation mit dem Fälschungs-Template ist. Vorzugsweise erfolgt diese Klassifikation anhand von Bildern und entsprechenden Differenzbildern, die im Zeitpunkt des Auflegens des Fingers erfasst wurden. Wird im Schritt 256 festgestellt, dass der Wert für das erste Template größer ist als der Wert für das zweite Template so wird zum Schritt 256 übergegangen, in dem der Fingerabdruck, ähnlich wie im Schritt 210 als echt klas-

25

30

35

sifiziert wird. Andernfalls wird im Schritt 260 der Fingerabdruck, ähnlich wie im Schritt 212, als nicht echt klassifiziert.

5 Gemäß einem bevorzugten Ausführungsbeispiel werden die Schritte 254 und 256, also die Korrelation und die anschließende Klassifikation, nur um den Zeitpunkt des Auflegens des Fingers durchgeführt, d. h. nur für die wenigen Bilder in der Sequenz in denen sich die aufeinanderfolgenden Bilder in ihrer Fläche deutlich unterscheiden, also z. B. nur für die Bilder 6 bis 10 in der Bildsequenz 100, die in Fig. 1A gezeigt ist. Gemäß einem weiteren bevorzugten Ausführungsbeispiel werden diese Bilder durch eine Schwerpunktsberechnung im Histogramm bestimmt. Nur dann, wenn der Schwerpunkt einen vorbestimmten Schwellenwert überschreitet, werden die Histogramme der Korrelation und Klassifikation zugeführt. Mit anderen Worten erfolgt zunächst eine vollständige Verarbeitung aller Bilder derart, dass für aufeinanderfolgende Bilder jeweils Differenzbilder erzeugt werden und erst anhand der Histogramme erfolgt dann die tatsächliche Auswahl derjenigen Differenzbilder die zur Korrelation und Klassifikation herangezogen werden.

Abhängig von dem Ergebnis des erfindungsgemäßen Verfahrens werden dann weitere Schritte eingeleitet oder nicht eingeleitet, z. B. der Zugriff auf geschützte Daten, das Öffnen von Türen und ähnliches. Wird z. B. festgestellt, dass ein Fingerabdruck von einer Fälschung stammt, wird ein Alarm oder ähnliches ausgelöst, um z. B. dem Werkschutz den Versuch eines unberechtigten Eindringens anzuzeigen.

Alternativ kann bei der Feststellung, dass der Fingerabdruck „echt“ ist, die erfasste Bildsequenz einer weiteren Verarbeitung zur Personen-Identifizierung zugeführt werden.

Patentansprüche

1. Verfahren zur Fälschungserkennung, mit folgenden Schritten:

5

(a) Erfassen (200) einer Bildsequenz (100), die eine Mehrzahl von Bildern (0-19) des zu erkennenden Fingerabdrucks umfasst;

10 (b) Bilden (202) zumindest eines Differenzbildes aus zwei Bildern der erfassten Bildsequenz (100);

(c) Erfassen (206) einer Textur in dem zumindest einen Differenzbild;

15 (d) Vergleichen (208) der Textur mit einer vorbestimmten Textur, um zu bestimmen, ob die erfasste Bildsequenz (100) von einem echten Finger oder von einem Imitat stammt.

2. Verfahren nach Anspruch 1, bei dem die Bildsequenz (100) beim Auflegen eines Fingers (104) auf eine Sensoreinheit (106) erzeugt wird und zeitlich aufeinanderfolgende Bilder (0-19) umfasst.

25 3. Verfahren nach Anspruch 1 oder 2, bei dem die Bilder (0-19) der erfassten Bildsequenz (100) als Grauwertbilder erfasst werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem eine Mehrzahl von Differenzbildern im Schritt (b) erzeugt wird, indem jeweils zwei aufeinanderfolgende Bilder der Bildsequenz (100) voneinander subtrahiert werden, wobei die zu subtrahierenden Bilder die Bilder sind, die in der erfassten Bildsequenz zum Zeitpunkt des ersten Kontakts zwischen Finger (104) und Sensoreinheit (106) angeordnet sind.

35

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem im Schritt (d) die im Schritt (c) erfasste Textur mit einer ers-

ten Textur für einen echten Finger und mit einer zweiten Textur für ein Imitat verglichen wird, um die erfasste Textur zu klassifizieren (254, 256, 258, 260).

- 5 6. Verfahren nach einem der Ansprüche 1 bis 5, bei dem der Schritt (d) folgende Schritte umfasst:

(d1) Filtern (250) des Grauwertdifferenzbildes, um ein Gradientenbild zu erhalten,

10

(d2) Berechnen (252) eines Histogramms des Gradientenbildes;

(d3) Korrelieren (254) des berechneten Histogramms mit einer ersten gegebenen Maske für einen echten Finger und mit einer zweiten gegebenen Maske für ein Imitat, und

15

(d4) Klassifizieren (256, 258, 260) der erfassten Bildsequenz (100) als von einem echten Finger stammend, wenn der Wert der Korrelation mit der ersten Maske größer ist als der Wert der Korrelation mit der zweiten Maske.

20

7. Verfahren nach Anspruch 6, bei dem die Schritte (d1) und (d2) für eine Mehrzahl von Differenzbildern durchgeführt werden, wobei das Verfahren vor den Schritten (d3) und (d4) folgende Schritte umfasst:

25

Berechnen eines Schwerpunkts in jedem Histogramm,

Vergleichen des Schwerpunkts mit einem Schwellenwert, und

30

Weiterleiten der Histogramme an die Schritte (d3) und (d4), deren Schwerpunkt den Schwellenwert übersteigt.

Zusammenfassung

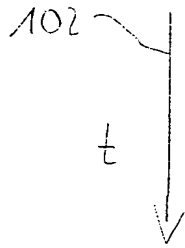
Verfahren zur Fälschungserkennung bei der Fingerabdruckerken-
nung unter Verwendung einer Texturklassifikation von Grau-
5 wertdifferenzbildern

Bei einem Verfahren zur Fälschungserkennung bei der Fingerab-
druckererkennung wird zunächst eine Bildsequenz (100) erfasst,
die eine Mehrzahl von Bildern (0-19) des zu erkennenden Fin-
10 gerabdrucks umfasst. Aus zumindest zwei Bildern wird ein Dif-
ferenzbild erfasst, indem eine Textur erfasst wird. Die Tex-
tur wird mit einer vorbestimmten Textur verglichen, um zu
bestimmen, ob die erfasste Bildsequenz (100) von einem echten
Finger oder von einem Imitat stammt.

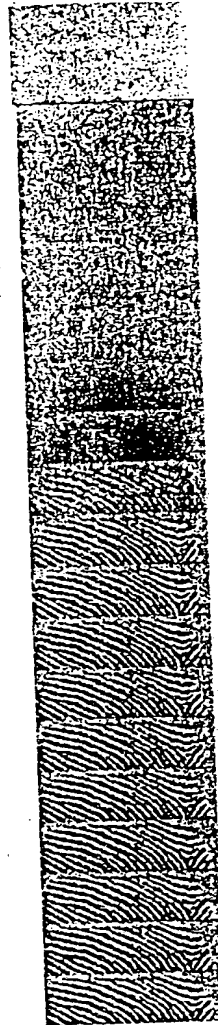
15

Figur 1A

Figur zur Zusammenfassung:



- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19



100

Fig. 1A

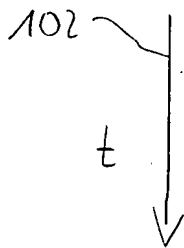
Bezugszeichenliste

0-19 Bilder

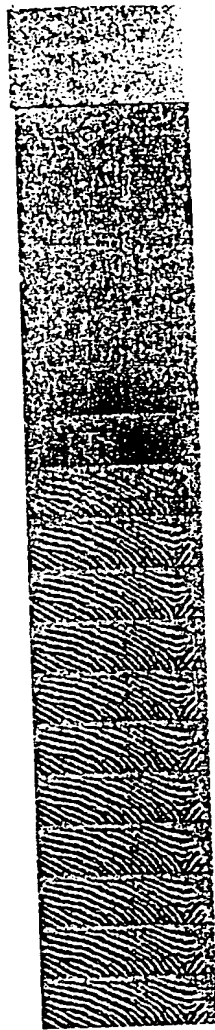
100	Bildsequenz
102	Pfeil
104	Finger
106	Sensoreinheit
200-212	Verfahrensschritte
220a	aktuelles Bild einer Bildsequenz von einem Originalfinger
220b	dem Bild 220a vorhergehendes Bild
220c	Differenzbild
230a	aktuelles Bild einer Bildsequenz von einer Folienfälschung
230b	dem Bild 230 vorhergehendes Bildsequenz
230c	Differenzbild
240a	aktuelles Bild von einer Bildfolge von einer Hauchfälschung
240b	dem Bild 240a vorhergehendes Bild
240c	Differenzbild
250-260	Verfahrensschritte

102

t



- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19

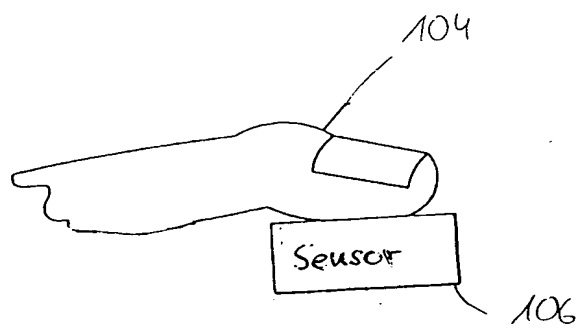


100



Fig. 1A

Fig. 1B



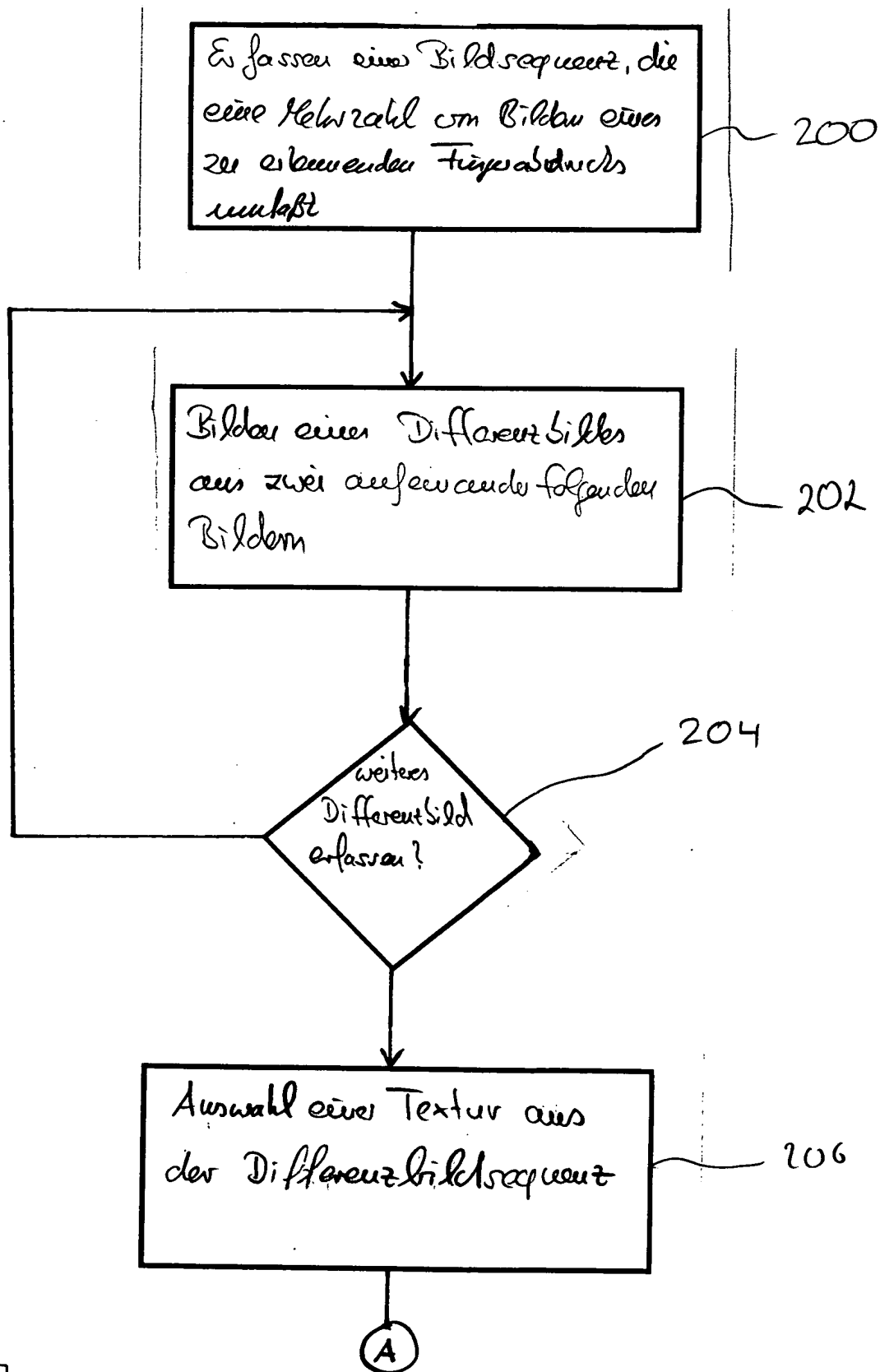


Fig. 2A

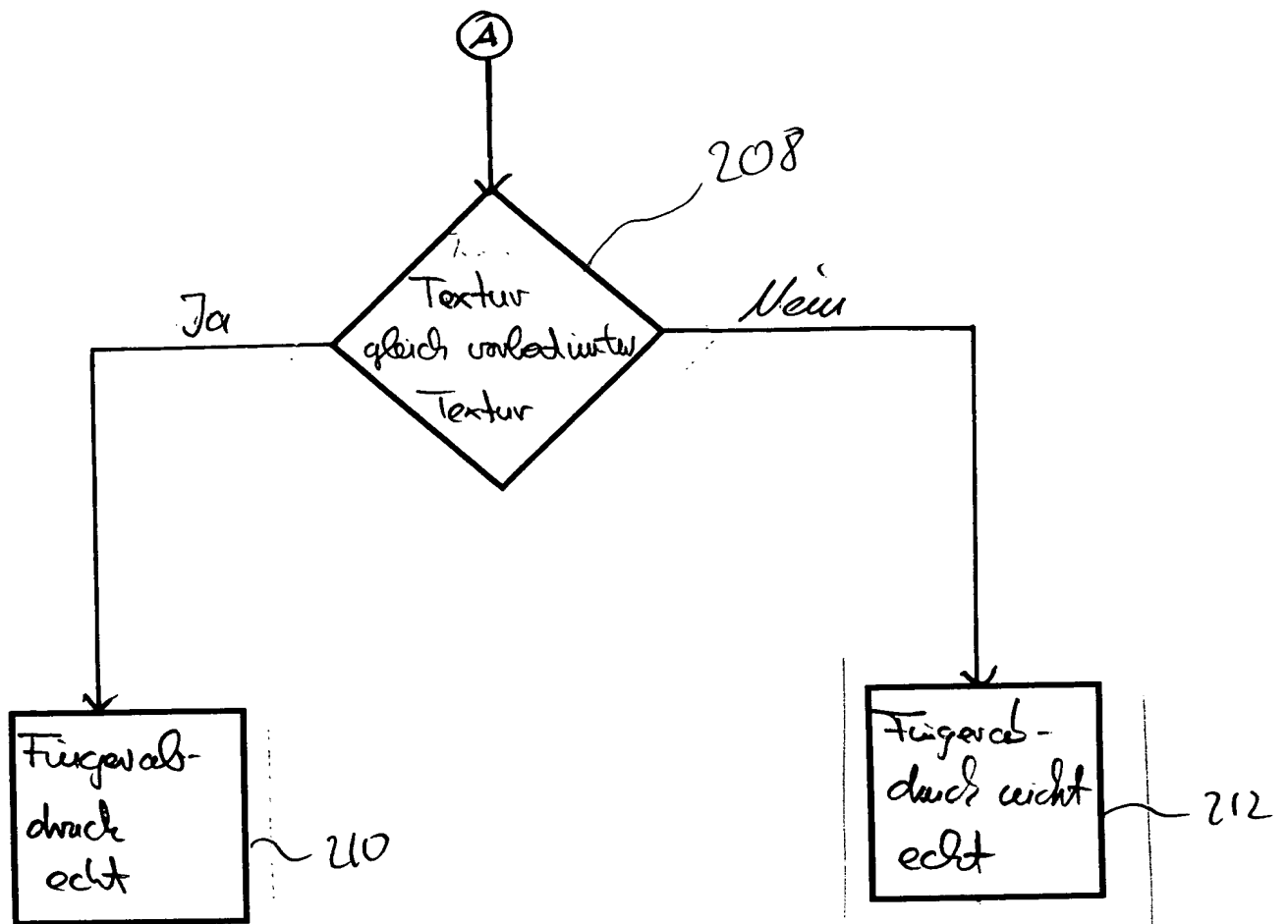


Fig. 2B

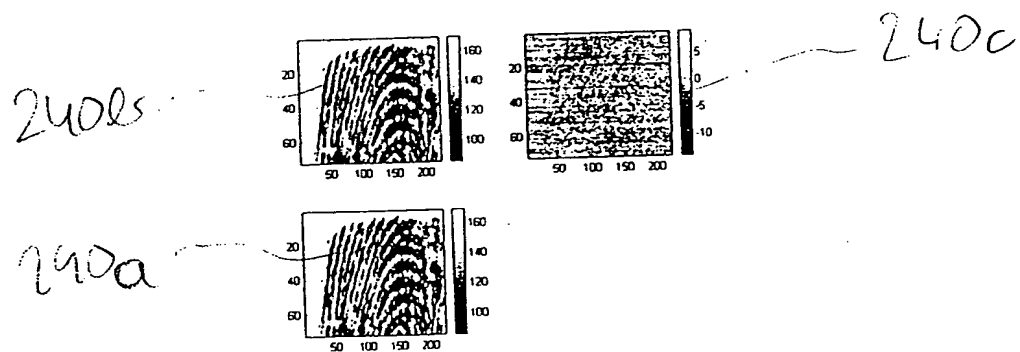
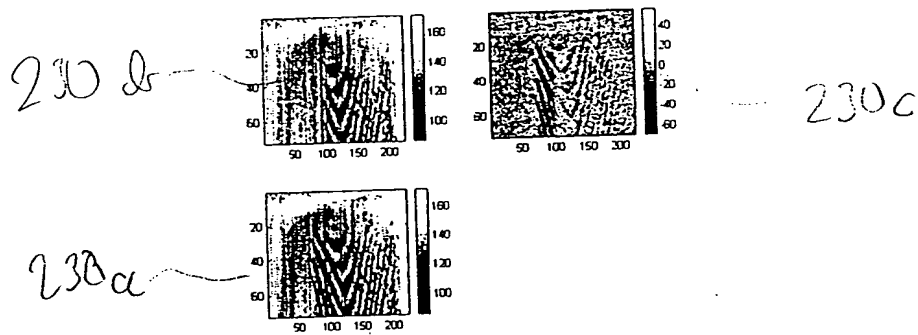
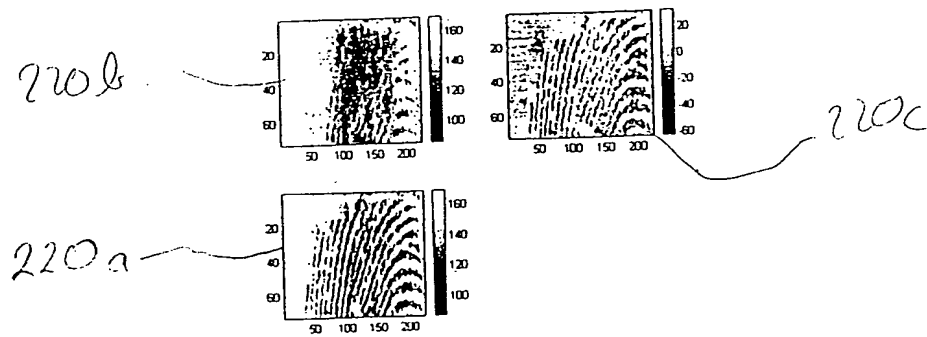


Fig. 3

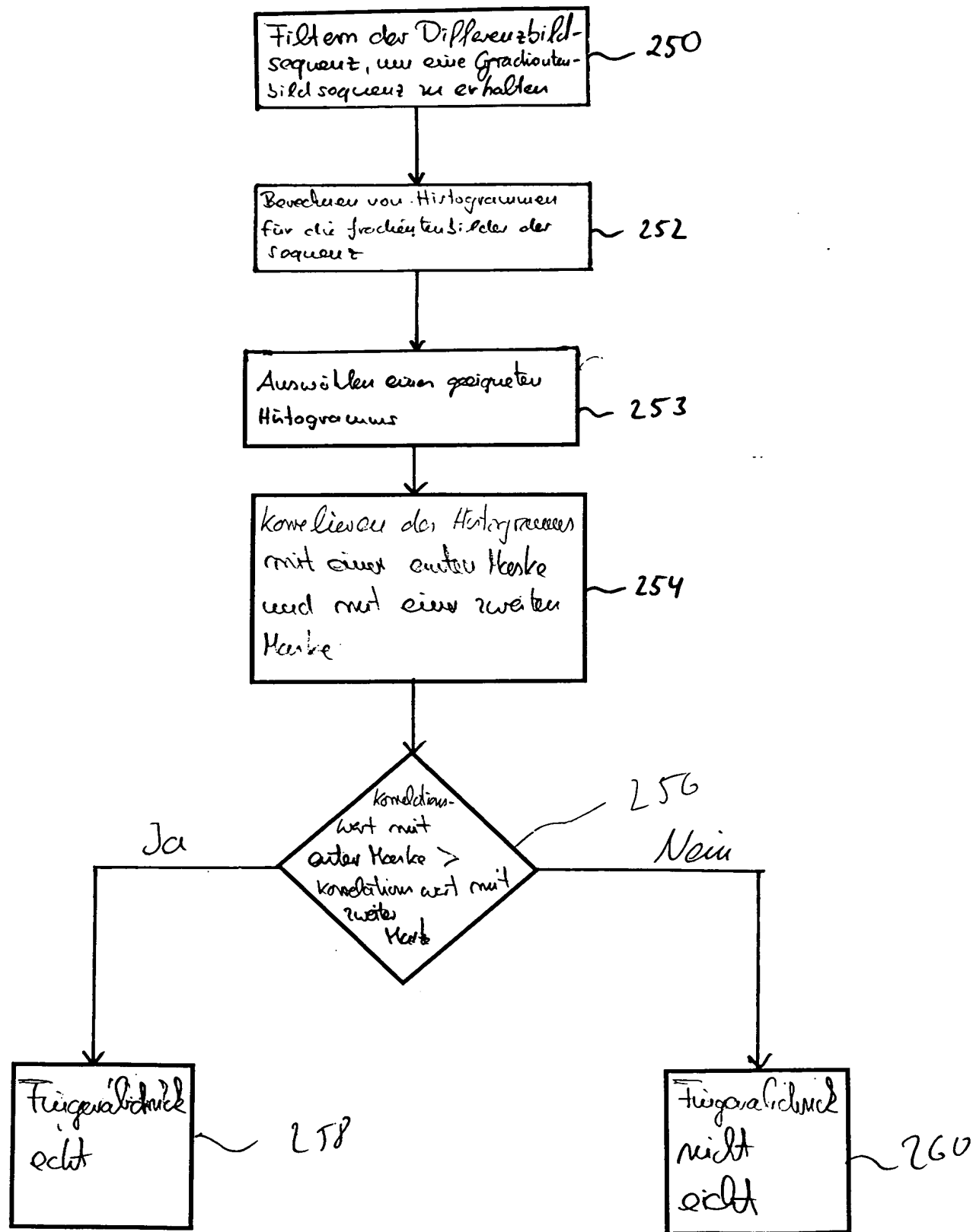


Fig. 4